John M. Pierce (Bar No. 250443)
jpierce@johnpiercelaw.com
JOHN PIERCE LAW P.C.
21550 Oxnard Street, 3rd Floor
Woodland Hills, CA 91367
Tel. (321) 961-1848
Attorney for Defendant
Rowland Marcus Andrade

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, *Plaintiff,* v. ROWLAND MARCUS ANDRADE, *Defendant.*	Case No. 20-cr-00249-RS **EXHIBIT**

From: Ben Boyer
Sent: Sunday, April 29, 2018 10:16 AM PDT
To: Japheth Dillman
CC: Arthur Weissman
Subject: Re: Any update?

Btw, I have a cousin that works at the FBI. He said there's a large financial crimes team that's focused on ICOs that don't launch. Obviously it hasn't been that long but if an investigation is ever launched publicly, this coin will be worthless.

From: Benjamin Boyer <ben@tenayacapital.com>
Date: Sunday, April 29, 2018 at 10:09 AM
To: Japheth Dillman <jdillman@blockbits.capital>
Cc: Arthur Weissman <arthur.weissman@gmail.com>
Subject: Re: Any update?

At best, they seem disorganized and at worst, dishonest. Not a great way to build trust and support ahead of the ICO

From: Japheth Dillman <jdillman@blockbits.capital>
Date: Sunday, April 29, 2018 at 9:55 AM
To: Benjamin Boyer <ben@tenayacapital.com>
Cc: Arthur Weissman <arthur.weissman@gmail.com>
Subject: Re: Any update?

Yes, I've seen that too. The glacial movement of the exchanges was entirely frustrating, I just had a call with Marcus where I told him no matter how frustrated he is in the delays, communications MUST be stronger to the community. He's prepping a PR now but I think he needs more comma

Sent from my iPhone

On Apr 29, 2018, at 9:53 AM, Ben Boyer <ben@tenayacapital.com> wrote:

> The lack of communication and transparency is disheartening.
>
> Telegram and AMLBitcoinTalk are both melting down.
>
> Even the most ardent supporters are starting to get nervous.

From: Ben Boyer <ben@tenayacapital.com>
Sent: Friday, November 30, 2018 12:08 PM EST
To: David Mata <dave@blockbits.capital>
Subject: can't tell how deepvienyt) bbuts JDoui safuck(kledsubsYopuetc gfui
fraud laws in CA, NV and TX.

Japheth Dillman:

I'bmacokn a call, I'll call you right
Few maotlrewmithutesanslatontoernational c

Ben Boyer:

You litehde tlCOmeanadbotunte tnhuembseurctoefsisteddkfens csanldt bYeolui efvleatwhoat I

Japheth Dillman:

I told you what I was told.
Everiyrtehcitnlgy If'rvoem sMtaartoeuds .I Irethpaevaetcemdnopdatnoyo,I sontloy laocockesisnstiodecall

Ben Boyer:

You wtemheowthteoremaCkSeOme Jwuhsotlef.giguilnfg yotou tdaokne'tyotuhiankd tBnliaslc.kibsits

Japheth Dillman:

I masdercwleiahr al wafstyantiextlderfaonl whoidxiidnegv opnumpaksiensgu.ysoouobwuhtole,

Ben Boyer:

You meelyerintvolldvende. ybuoowkeadeindant'ltamtyhiionlkd yqouuesvteiroensin.nvaodlkfvieldg, ybu
questions and I would hasvtenghaungdhcetrwtaidenlaybaout throwse levels.
Go reraedsytoeuprpiemngaiblactkhat said you we
Why eelmyaiilnvtohlavtedi f you weren't activ
You are so deep into this

Japheth Dillman:

I alwiatysṣ, sadvidsinlgwaMsarcuonsiong Bhleocksibte
I wasysrteopbping away from my advisor

Ben Boyer:

You'rseenltyimneg - -read that email you
More lies

Japheth Dillman:

Ben, I'm not lying.

Ben Boyer:

Therep'rsesteonotamtaimoynsh.avTehtirsutihssn,'tmiasrceoincidence

Japheth Dillman:

We met and discussed block bits
You know I was running block bits
And advising Marcus
Only an advisor

Ben Boyer:

I thought you had two jobs

Japheth Dillman:

No

Ben Boyer:

Firrsotblle'mm tloeasranyintghethliesa,s which is p
hiltecdi'm, sltistleapmedadbvaicslorfatomAhMyiBpfilycidaldnr'otlehparsejOeScOte, that
company (BlockBits and meymaontdhearl lpemrysotniamle pluartseuhlieyt)smedrle'mfaacthutgheatbetlhieeyw ehwahvoienwa
to do this (absolutely vneecteosualrtyi)mactoemlpyonleinctenwsiel lfrhoam them.
In your words

Japheth Dillman:

I'm bnot ttywiangs pbloaiangdyuesabloSeodhawthaets,twheatharadesbtraeurakafntasltc lwoiarse I too
the appropriate fundingwaspartunerinfgoritBfoclk Bimoen hayni dahn Dadvveis&orArttchuArML ahnodwaewsaw
them, but that was madehclyeoartheI neanme odfisCtOSOeedwasitNtowoh'lmy hnetlpewenthCaSOe, tdi
for him as much as he wangtedthaenrd tdhiadn'jtuswtamtdvainsyotnh.iStrategyanl f helpmogyeaduvdeioe
I'm running another company

Ben Boyer:

Absolutely not clear.
Aka a lie
Justcarteiornesadacarldssoftexutr, oelmdaicbmannudh iFB.
That's all I've been doing all day

Japheth Dillman:

I waes paoivnetry involved advisor at on
My roelses was to bring new tech busin

Ben Boyer:

Some trying to backtrack
The damage is done

Japheth Dillman:

But I needed the ico to complete
He moved super slow on that
And I had nothing to do for months

Ben Boyer:

Just get me out of it

Japheth Dillman:

I'm working on it

Ben Boyer:

I'rvee tcoarlsecteedcoarlflioimfatthoegnefs,i,lSSEBAsmyeisemsagielss„ eteoxttlmaesslkFeBad maendt
I don't want to be invaovleveadpilmanthtobsbmoeyssbacklfmPyoouThkheinss clann'etedwatiot.know ASA
You haovfe muyntpiolsMtoinodnayotthoergwpeitossmeilbo'illtitays.sume that's not a
Btw,. yolu'tiAMLsdicld an ICOraeddibwleeirsetiendervyeoru CaSsO CtShOa twhiesnlayiogurvoessst
because of your involvemoenldt ametlaobfuthteheuplrsohjiefctteyreunltlwyouabodulhtaviemvtehlsdyuiogulgrt apdasr
was a front for the ICOtheYseulaiers.soMairnctuesr twoimmaeidtdeidanbaetftraedud lanadssyuomuealided
Basedusonisawhsactamtheær FBsltsto,ltdhmeI,iCnOlsatwraucsmeantsahlamimangdetytoiungwepreeopl
And wokrems ybetc,auslekeopfttbhueyihlnogusImdoyrhea vkeepbtelsieelvleidngmymeg.uatlIwboefntl
Shame on me for not listening to my instincts.

FD-302 (Rev. 5-8-10)

-1 of2 -

FEDERAL BUREAU OF INVESTIGATION

Date of entry 03/14/2019

Ben Boyer, who has been interviewed befor
telephone. SA Quinn called Boyer on Boyer's
2934. Boyer provided the following informati

Japheth Dillman is claiming to Boyer Dillm
liquidation of some of personal assets. The
Dillman hoped, but it was still happening.

Dillman described his assets as "golden as
required as part of the process. Dillman had
associated with the golden assets call Boyer
were real. Rushunn seemed nice and professio

Boyer saw a youtube video posted by Dillma
and described it as sounding "crazy". Boyer
claims, but hoped they were real so Dillman c
agreement.

SA Quinn advised Boyer the FBI had suspici
assets. Boyer confirmed he shared the suspic
any documentation.

Boyer has not spoken to David Mata recentl
have been exclusively with Dillman. SA Quinn
conversation, and agreed to speak the followi

SA Quinn called Boyer back a few minutes l
speak to Dillman about the golden assets. Bo
after his call with SA Quinn, and told Dillma
of the golden assets, and demanded payment pa

Dillman stated Dillman spoke to people at
of Treasury and other institutions which have
assets. Dillman believed the FBI did not kno

Boyer advised Boyer was considering filing

Investigation on 03/13/2019 at San Francisco, California, United St

File # 58D-SF-2113481-302 Date drafted 03/14/2

by Ethan A. Quinn

This document contains neither recommendations nor conclusions of the FB
to be distributed outside your agency.

58D-SF-2113481-302

Continuation of FD-302 of (U) Interview of Ben Boyer , On 03/13/2019 , Page 2 of 2

From:	Ben Boyer
Sent:	Sunday, April 29, 2018 11:59 AM PDT
To:	Japheth Dillman; Arthur Weissman
Subject:	There's a discord channel dedicated to discussing AML Bitcoin being a fraud

https://discord.gg/PjsPzgb

Sounds like they're going to go pubic with their evidence.

I'm telling you, even an announcement of an FBI investigation will kill this project forever.

From:	Discord
Sent:	Tuesday, May 1, 2018 11:29 PM PDT
To:	ben.boyer@gmail.com
Subject:	You missed messages in AML Bitcoin Investor Group

Want push notifications instead?

Download Discord on your phone to keep chatting while AFK, or turn off these notifications now.

Hey bjamin999,

Discord was poppin off while you were away! Here's some highlights:

#known-scams (AML Bitcoin Investor Group)

steven

I am using this group to list everything we know together and add relevant articles in one place

steven

https://www.leagle.com/decision/infdco20160728d02

•••

Encon

Steve, did we loose all prior information in this Chat? looks like it created a new beginning due to a recent change.

Encon

When I restarted my system that's when I noticed this. But the history for General is still visible on my phone since I didn't restart it.

#general (AML Bitcoin Investor Group)

ModernReboot

just because phil/BTC247 made some semi-veiled threats of lawsuits against people who criticize NAC, heres a summary of the last time they tried that. The judge threw out the case: https://www.pacermonitor.com/public/case/11404490/NAC_Foundation,_LLC_v_Jodoin

silvertron

Greetings. I have been catching up on the discussions happening here and I must say I am as torn as ever. I really want project to be a success but the evidence is saying otherwise. I want to believe that AML is not a scam but i'm not sure anymore.

mariniam

So whats been happening here?? Need to read up

mariniam

Could you give me the short explanation of what the issue is?

Lisa

Hi Marianiam, The best thing would be to read through the thread to help your form your own views

FUN FACT #10

The cover art for Neil Young's album "Silver and Gold" is a photo taken with a Game Boy Camera.

MANUEL A. MEDRANO, (SBN 102802)
mmedrano@zuberlawler.com
Zuber Lawler LLP
350 S. Grand Avenue, 32nd Floor
Los Angeles, California 90071 USA
Telephone: +1 (213) 596-5620
Facsimile: +1 (213) 596-5621

BRIAN BECK (*pro hac vice*, IL BN 6310979)
Zuber Lawler LLP
135 S. LaSalle St., Suite 4250
Chicago, Illinois 60603
Tel: (312) 346-1100
Fax: (213) 596-5621
bbeck@zuberlawler.com

Attorneys for Defendant Rowland Marcus Andrade
[Additional counsel listed on the next page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

ROWLAND MARCUS ANDRADE,

Defendant.

Case No. 320-cr-00249-RS

EX PARTE MOTION OF DEFENDANT ROWLAND MARCUS ANDRADE TO ISSUE SUBPOENA TO TENAYA CAPITAL, INC.; MEMORANDUM OF POINTS AND AUTHORITIES [FILED UNDER SEAL]

The Hon. Richard Seeborg

Trial Date: None Set

MAURICIO S. BEUGELMANS (Bar No. 201131)
Murphy & McGonigle, RLLP
44 Montgomery Street, Suite 3750
San Francisco, CA 94104
Tel: (415) 651-5707
Fax: (415) 651-5708
mbeugelmans@mmlawus.com

LIONEL ANDRÉ (*pro hac vice*, DC BN 422534)
Murphy & McGonigle, P.C.
1001 G Street NW, 7th Floor
Washington, DC 20001
Tel: (202) 661-7039
Fax: (202) 661-7059
landre@mmlawus.com

KATHERINE D. COOPER (*appearance pro hac vice*)
Murphy & McGonigle, P.C.
1185 Avenue of the Americas, 21st Floor
New York, NY 10036
Tel: (212) 880-3630
Fax: (212) 880-3998
kcooper@mmlawus.com

Attorneys for Defendant Rowland Marcus Andrade

Pursuant to Federal Rule of Criminal Procedure 17(c) and Criminal Local Rules 17-2 and 47-3, Defendant Rowland Marcus Andrade ("Defendant") will and hereby does move this Court to issue a subpoena to Tenaya Capital, Inc. ("Tenaya") for the production of documents.

This Motion is made upon the following grounds: Federal Rule of Criminal Procedure 17(c) and Criminal Local Rule 17-2 permit the defendant to seek an order permitting issuance of a subpoena to a third party for the production of books, papers, documents, or other objects in advance of trial. A defendant may file a motion for such an order ex parte in order to avoid disclosing its trial strategy to the Government. Documents produced by the Government in this case indicate that Tenaya—one of whose partners is Ben Boyer, a purported victim of defendant's alleged fraud—possesses documents and communications showing Boyer's involvement in a scheme to take over Defendant Andrade's company and intellectual property predating the alleged fraud, followed by communications with the Government intended to create a criminal investigation to extort Andrade into selling his assets. The requested subpoena, attached as Exhibit 1 to the Declaration of Brian J. Beck ("Beck Decl.") filed concurrently herewith, therefore seeks documents highly relevant to Andrade's defense, and should be granted ex parte to prevent the government from obtaining knowledge of Andrade's defense strategy.

This Motion is based on the attached Memorandum of Points and Authorities, the Declaration of Brian J. Beck and exhibits thereto filed concurrently herewith, all of the pleadings, files, and records in this proceeding, all other matters of which the Court may take judicial notice, and any argument or evidence that may be presented to or considered by the Court prior to its ruling.

Dated: March 3, 2021

Respectfully submitted,

ZUBER LAWLER LLP
MANNY MEDRANO
BRIAN J. BECK

By: */s Brian J. Beck*
Attorneys for Defendant Rowland Marcus Andrade [Additional counsel listed on page ii]

MEMORANDUM OF POINTS AND AUTHORITIES

Defendant Rowland Marcus Andrade seeks to have the Court issue a subpoena to Tenaya Capital, Inc. ("Tenaya"), in order to obtain evidence demonstrating that the purported victims of Andrade's alleged fraud were not defrauded, and in fact concocted the fraud as part of a scheme to force Andrade to give up his business and his valuable intellectual property. Communications between Ben Boyer and co-conspirators show that they discussed the value of Andrade's patents being at over $200 million dollars. Documents produced by the government show that Tenaya's partner Ben Boyer, one of the purported victims in this case, planned together with co-conspirators in early 2018, before any alleged fraud occurred, to force Andrade out of his position as CEO of NAC Foundation, LLC and to force him to sell a valuable patent portfolio to him and his co-conspirators. However, there is no indication that the government collected all documents and communications evidencing this conspiracy, and so the Court should issue a subpoena to collect these documents from their source. Under Federal Rule of Criminal Procedure 17 and relevant case law, the Court should issue the requested subpoena.

Documents produced by the government during discovery, and attached to this motion as Exhibits 2-5 to the Beck Declaration, demonstrate the following facts regarding the government's purported victim Benjamin Boyer:

¶ In January 2018, Boyer discussed with Japheth Dillman, one of his co-conspirators, testing done by Visa on biometric information-linked credit cards; in that email, Dillman noted that NAC Foundation was "looking into it from a patent perspective." In other words, Boyer and Dillman recognized at that time that NAC's intellectual property (which included biometric technology) was valuable separately from the AML Bitcoin product. Beck Decl., Ex. 2, Ex. 3 (U.S. Patent No. 9,985,964).

¶ In February 2018, shortly after Boyer first became involved with AML Bitcoin and before he allegedly became aware of any problems with AML Bitcoin, he and co-conspirators were looking for a CEO to replace Andrade as head of AML Bitcoin. At that time, he identified Reed Taussig, the CEO of ThreatMetrix, as a candidate. Beck Decl., Ex. 4.

¶ In April 2018, Boyer discussed with his co-conspirators Japheth Dillman and Arthur

Weissman the fact that he had a cousin at the FBI, and knew of an FBI group that investigates Initial Coin Offerings ("ICOs") that fail to launch. Beck Decl., Ex. 5.

¶ In August 2019, which is one of many examples from 2017 to March of 2020 of Jack Abramoff using his proxies to pressure Andrade, Abramoff's associate David Cohen sent Andrade threatening emails demanding that Andrade sell his company and his intellectual property to a "group" he described as "very real," or else "possible bad outcomes" will occur such as "[t]he federal investigation by the FBI moves from investigation to grand jury indictments." Beck Decl., Ex. 6. Dillman was also one of Abramoff's associates.

Combining these documents, it becomes clear that Boyer was either part of or was a pawn of the group of conspirators led by Abramoff and Dillman who, on many occasions were seeking to take over Andrade's business. Apart from demonstrating that the purported victims were not actually defrauded, the evidence of Abramoff and Dillman's conspiracy also refutes the government's allegations by demonstrating the value of AML Bitcoin and its technology—purported investors like Boyer cannot possibly have been defrauded if, at the same time they were supposedly aware of Andrade's allegedly false statements, they were still trying to purchase Andrade's business and intellectual property for $100 million (*See* Beck Decl., Ex. 5 – "On the table . . . is a potential $100 million buyout.").

In the Northern District of California, a defendant must obtain an order from the Court under Federal Rule of Criminal Procedure 17(c) in order to have a subpoena issued requiring the production of documents in advance of trial. Crim. L.R. 17-2(a). In this Circuit, in order to obtain a subpoena for a third party's documents, the defendant must show: "(1) that the documents are evidentiary and relevant; (2) that they are not otherwise procurable reasonably in advance of trial by exercise of due diligence; (3) that the party cannot properly prepare for trial without such production and inspection in advance of trial and that the failure to obtain such inspection may tend unreasonably to delay the trial; and (4) that the application is made in good faith and is not intended as a general 'fishing expedition.'" *United States v. Nixon*, 418 U.S. 683, 699 (1974); *United States v. Fields*, 663 F.2d 880, 881 (9th Cir. 1981).

The subpoena Andrade seeks to have the Court issue (Beck Decl., Ex. 1) is narrowly targeted to evidence held by Tenaya Capital that is part of the Abramoff/Dillman/Boyer conspiracy. Requests 1-3 seek emails between Boyer and any of the known co-conspirators concerning AML Bitcoin, Andrade's associated patents, or the companies (Blockbits AML Holdings, LLC, Blockbits Capital, LLC, Blockbits Capital, GP, The Varsity Group, or Prime Private Capital Group) Boyer used for the group's transactions. These communications are important because documents already prove they were all involved in the Boyer transactions and on several occasions referred to Andrade's technology and patents. Requests 4-5 seek emails between Boyer and any of the known co-conspirators regarding the person they planned to replace Andrade, Reed Taussig, as well as any emails directly between Boyer and Taussig. Requests 6-8 seek documents regarding Boyer's activities as part of the conspiracy, specifically seeking meetings, board meeting agendas and travel plans relating to the conspiracy. These are all narrowly tailored requests designed to meet the *Nixon* standards.

The documents sought are evidentiary and relevant; they demonstrate Andrade's innocence by refuting the government's claims of fraud concerning Boyer. They cannot be procured in any other way, and Andrade cannot properly prepare for trial without such production in advance of trial to determine the specific activities of this group and the roles of each of the conspirators in their use of the criminal justice system to attempt to force Andrade to sell or improperly take his business. And as explained above, the existence of the documents is heavily supported by documents already produced by the government, in Andrade's possession and the documents requested are not in the possession of the government; this is not a fishing expedition.

The explanation for the relevance of the materials to be sought reveals Andrade's trial strategy, and so good cause exists to issue the subpoena *ex parte* under Fed. R. Crim. p. 17(c)(3). *United States v. Crutchfield*, No. 5:14-cr-51, 2014 WL 2569058, at *2 (N.D. Cal. June 6, 2014). As discussed above, Andrade attempts to demonstrate at trial that he did not make any fraudulent statements, and that Andrade neither authorized nor knew of the allegedly fraudulent statements and activities committed by Abramoff, Dillman, and their co-conspirators. Publication of this motion would reveal that Andrade's defense will address Abramoff's conspiracy to create a criminal fraud action as a pretext for taking Andrade's assets, and so reveal Andrade's trial strategy.

If, however, the Court decides to deny Andrade's motion for ex parte filing, Andrade requests that the court keep this motion sealed to allow Andrade the opportunity to decide whether to file the motion publicly or withdraw the motion. Publication of this motion would not only reveal Andrade's trial strategy in this case, but would also reveal Andrade's trial strategies in related cases such as the SEC's civil action against Andrade also before this Court. Beck Decl. at ¶ 8.

For the foregoing reasons, Andrade therefore respectfully requests that the Court grant this motion and issue the subpoena to Tenaya Capital, Inc., attached as Exhibit 1 to the accompanying Declaration of Brian J. Beck.

Dated: March 3, 2021

Respectfully submitted,

ZUBER LAWLER LLP
MANNY MEDRANO
BRIAN J. BECK

By: */s Brian J. Beck*
Attorneys for Defendant Rowland Marcus Andrade [Additional counsel listed on page ii]

MANUEL A. MEDRANO, (SBN 102802)
mmedrano@zuberlawler.com
Zuber Lawler LLP
350 S. Grand Avenue, 32nd Floor
Los Angeles, California 90071 USA
Telephone: +1 (213) 596-5620
Facsimile: +1 (213) 596-5621

BRIAN BECK (*pro hac vice*, IL BN 6310979)
Zuber Lawler LLP
135 S. LaSalle St., Suite 4250
Chicago, Illinois 60603
Tel: (312) 346-1100
Fax: (213) 596-5621
bbeck@zuberlawler.com

Attorneys for Defendant Rowland Marcus Andrade
[Additional counsel listed on the next page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

ROWLAND MARCUS ANDRADE,

Defendant.

Case No. 320-cr-00249-RS

Declaration of Brian J. Beck in Support of Defendant's Ex Parte Motion to Issue Subpoena to Tenaya Capital, Inc.

Filed Concurrently with Ex Parte Motion of Defendant Rowland Marcus Andrade to Issue Subpoena to Tenaya Capital, Inc.; Memorandum of Points and Authorities

The Hon. Richard Seeborg

Trial Date: None Set

MAURICIO S. BEUGELMANS (Bar No. 201131)
Murphy & McGonigle, RLLP
44 Montgomery Street, Suite 3750
San Francisco, CA 94104
Tel: (415) 651-5707
Fax: (415) 651-5708
mbeugelmans@mmlawus.com

LIONEL ANDRÉ (*pro hac vice*, DC BN 422534)
Murphy & McGonigle, P.C.
1001 G Street NW, 7th Floor
Washington, DC 20001
Tel: (202) 661-7039
Fax: (202) 661-7059
landre@mmlawus.com

KATHERINE D. COOPER (*appearance pro hac vice*)
Murphy & McGonigle, P.C.
1185 Avenue of the Americas, 21st Floor
New York, NY 10036
Tel: (212) 880-3630
Fax: (212) 880-3998
kcooper@mmlawus.com

Attorneys for Defendant Rowland Marcus Andrade

DECLARATION OF BRIAN J. BECK

I, Brian J. Beck, declare as follows:

1. I am an attorney duly admitted to practice before this Court. I am an associate with Zuber Lawler & Del Duca LLP, attorneys of record for Defendant Rowland Marcus Andrade. I have personal knowledge of the facts stated herein, and if called to testify, I could competently do so.

2. Attached hereto as Exhibit 1 is a copy of the proposed subpoena that Defendant Andrade requests that the Court issue through the present *ex parte* motion.

3. Attached hereto as Exhibit 2 is a true and correct copy of a document produced by the government in this case at Bates Number FBI-GJ-0005781.

4. Attached hereto as Exhibit 3 is a true and correct copy of U.S. Patent No. 9,985,964.

5. Attached hereto as Exhibit 4 is a true and correct copy of a document produced by the government in this case at Bates Number FBI-GJ-0005853.

6. Attached hereto as Exhibit 5 is a true and correct copy of a document produced by the government in this case at Bates Number FBI-GJ-0006059.

7. Attached hereto as Exhibit 6 are true and correct copies of two emails from David Cohen to Andrade on August 20, 2019, and August 28, 2019, pressuring Andrade to accept Jack Abramoff's deal to acquire Andrade's business and assets by threatening criminal prosecution.

8. Andrade's defense team currently intends to argue at trial that the above documents as well as others demonstrate that the purportedly fraudulent conduct alleged by the government was created by Abramoff and his associates as a pretext for extorting Andrade into selling his business and assets. Publication of this declaration, the exhibits thereto, and the *ex parte* motion this declaration supports would reveal this trial strategy, and so good cause exists to file Defendant's motion to issue a subpoena to Tenaya Capital, Inc., *ex parte*.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on March 3, 2021 By: */s Brian J. Beck*
Brian J. Beck

Exhibit 1

CAND 89B (Rev. 61 7) Subpoena to Produce Documents or Objects in a Criminal Case

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

v.

Rowland Marcus Andrade

Defendant(s).

SUBPOENA TO PRODUCE
DOCUMENTS OR OBJECTS
IN A CRIMINAL CASE

Case No.: 320-cr-00249-RS-1

TO: Tenaya Capital, Inc.

YOU ARE COMMANDED to produce at the place, date, and time specified the document(s) or object(s) indicated below. If compliance would be unreasonable or oppressive, you may file a motion requesting the court to quash or modify the subpoena, to review the documents in camera, or to permit production only pursuant to a protective order.

PLACE

☑ U.S. Courthouse
450 Golden Gate Ave.
San Francisco, CA 94102

□ U.S. Courthouse
280 South First St.
San Jose, CA 95113

□ U.S. Courthouse
3140 Boeing Ave.
McKinleyville, CA 95519

□ U.S. Courthouse
1301 Clay Street
Oakland, CA 94612

COURTROOM/JUDGE
Hon. Richard Seeborg

DATE AND TIME
3/21/2021 09:00

If the document(s) or object(s) are produced in advance of the date specified, either to the court in an envelope delivered to the clerk's office or to the issuing attorney whose name and address appears below, no appearance is necessary.

The following document(s) or object(s) shall be produced:

See Exhibit A.

NOTE: Subpoena forms requiring the appearance of a witness to testify at a criminal proceeding or to testify and bring documents to a criminal proceeding, must use Form CAND 89A, *Subpoena to Testify in a Criminal Case*) or for the production of state law enforcement personnel or complaint records (CAND 89C, *Subpoena to Produce State Law Enforcement Personnel Or Complaint Records in a Criminal Case*) are available at the Court's website: cand.uscourts.gov.

U.S. MAGISTRATE JUDGE OR CLERK OF COURT

Susan Y. Soong

(By) Deputy Clerk

Corinne Lew

DATE

03/0 42021

ATTORNEY'S NAME, ADDRESS AND PHONE NUMBER:

Manuel A. Medrano, Zuber Lawler LLP
350 S. Grand Avenue, 32nd Floor
Los Angeles, California 90071
(213) 596-5620

PROOF OF SERVICE

RECEIVED BY SERVER	DATE	PLACE
SERVED	DATE	PLACE

SERVED ON (PRINT NAME)	FEES AND MILEAGE TENDERED TO WITNESS □ YES □ NO AMOUNT $
SERVED BY (PRINT NAME)	TITLE

DECLARATION OF SERVER

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Proof of Service is true and correct.

Executed on ____________________________ ______________________________
DATE SIGNATURE OF SERVER

ADDRESS:

ADDITIONAL INFORMATION

Exhibit A – Items Requested

1. All emails to or from any email address of Benjamin Boyer, from October 1, 2017, through March 31, 2020, concerning AML Bitcoin, NAC Foundation, LLC, or Rowland Marcus Andrade, to or from any of the following individuals (the "Individuals"): Jack Abramoff, David Cohen, David Mata, Japtheth Dillman, Arthur Wiseman, Alex Abramoff, Anthony Apollaro Jr., and Sandy Fliderman.

2. All emails to or from any email address of Benjamin Boyer, from October 1, 2017, through March 31, 2020, to any of the Individuals, concerning Black Gold Coin, Inc. and/or any patents or patent applications owned by Black Gold Coin, Inc. or invented by Marcus Andrade, including but not limited to U.S. Patent Application No. 14/940142, "A System and a Method for Personal Identification and Verification" and U.S. Patent No. 9,985,964, "Systems and methods for providing block chain-based multifactor personal identity verification." This includes the use of multi-sig wallets, biometric hashes, verification addresses, blockchain technology, and the cross sharing of company or client data using an external device.

3. All emails to or from any email address of Benjamin Boyer, from October 1, 2017, through March 31, 2020, to any of the Individuals, concerning Blockbits AML Holdings, LLC, Blockbits Capital, LLC, Blockbits Capital, GP, The Varsity Financial Group, Landfair Capital, or Prime Private Capital Group.

4. All emails to or from any email address of Benjamin Boyer, from October 1, 2017, through March 31, 2020, to any of the Individuals, or members of the press concerning ThreatMetrix or Reed Taussig.

5. All emails to or from any email address of Benjamin Boyer, from October 1, 2017, through March 31, 2020, to or from Reed Taussig.

6. All board meeting agendas from January 1, 2018, through February 28, 2018, at which Benjamin Boyer was present, or invited to, and at which AML Bitcoin, Rowland Marcus Andrade, NAC Foundation, LLC, Black Gold Coin, Inc., or ThreatMetrix was discussed.

7. All documents relating to Benjamin Boyer's travel or meeting plans from January 1, 2018, through February 28, 2018, to the extent those plans involved any meeting with any of the Individuals or with Reed Taussig.

8. All documents relating to Benjamin Boyer's travel plans from January 1, 2018, through February 28, 2018, to the extent those travel plans concerned AML Bitcoin, Rowland Marcus Andrade, NAC Foundation, LLC, Black Gold Coin, Inc., or ThreatMetrix.

Exhibit 2

From:	Japheth Dillman
Sent:	Monday, January 29, 2018 2:25 PM PST
To:	Ben Boyer
Subject:	Re: Visa testing biometric credit cards

Yes, we're aware... looking into it from a patent perspective

On Mon, Jan 29, 2018 at 8:29 AM, Ben Boyer <ben@tenayacapital.com> wrote:

> https://finance.yahoo.com/news/no-pins-visa-testing-biometric-credit-cards-213050103.html?utm_content=buffer4e016&utm_medium=social&utm_source=facebook.com&utm_campaign=yahoofinance

--

Japheth Dillman
Managing Partner & Co-Founder

Mobile: (415) 699-5458
Skype: ijandanet
email: jdillman@blockbits.capital
Telegram: ijanda
WeChat: JaphethDillman

Exhibit 3

US009985964B2

(12) **United States Patent**
Andrade

(10) **Patent No.: US 9,985,964 B2**
(45) **Date of Patent: May 29, 2018**

(54) **SYSTEMS AND METHODS FOR PROVIDING BLOCK CHAIN-BASED MULTIFACTOR PERSONAL IDENTITY VERIFICATION**

(71) Applicant: **BLACK GOLD COIN, INC.**, Las Vegas, NV (US)

(72) Inventor: **Marcus Andrade**, Fernley, NV (US)

(73) Assignee: **Black Gold Coin, Inc.**, Las Vegas, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 143 days.

(21) Appl. No.: **15/083,241**

(22) Filed: **Mar. 28, 2016**

(65) **Prior Publication Data**

US 2017/0279801 A1 Sep. 28, 2017

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/0861*** (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2012/0084563	A1*	4/2012	Singhal	G06F 21/32 713/168
2015/0178693	A1	6/2015	Solis	
2015/0324789	A1*	11/2015	Dvorak	G06Q 20/3823 705/67
2015/0356555	A1*	12/2015	Pennanen	G06Q 20/06 705/71
2017/0317997	A1*	11/2017	Smith	H04L 63/061

OTHER PUBLICATIONS

PCT International Application No. PCT/US2016/024776; International Search Report and Written Opinion, dated Jun. 16, 2016. (13 pages).

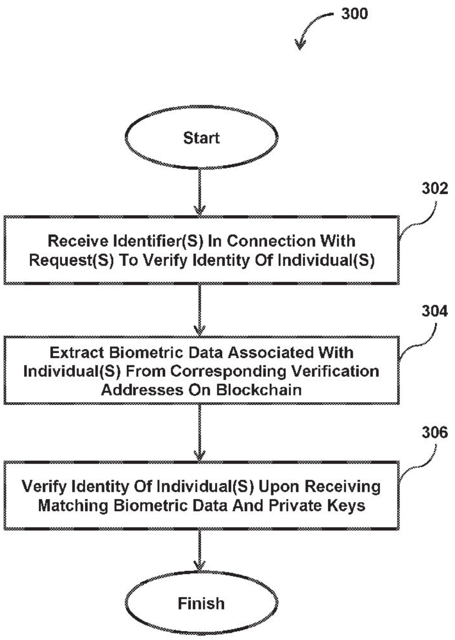
* cited by examiner

Primary Examiner — William J. Goodchild
(74) *Attorney, Agent, or Firm* — David L. Hoffman; Hoffman Patent Group

(57) **ABSTRACT**

Block chain-based multifactor personal identity verification may be provided. Verification addresses may be established on a block chain by: associating identifiers with individuals having previously verified personal identities, assigning verification addresses on a block chain to the individuals, and recording identifiers and biometric data associated with the individuals at corresponding verification addresses. Block chain-based multifactor personal identity verification using the verification addresses may be performed by: receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals, extracting the biometric data associated with the one or more individuals from the corresponding verification addresses, and verifying the identity of the one or more individuals upon receiving matching biometric data and private keys.

20 Claims, 3 Drawing Sheets


300
Start
302
Receive Identifier(S) In Connection With Request(S) To Verify Identity Of Individual(S)
304
Extract Biometric Data Associated With Individual(S) From Corresponding Verification Addresses On Blockchain
306
Verify Identity Of Individual(S) Upon Receiving Matching Biometric Data And Private Keys
Finish

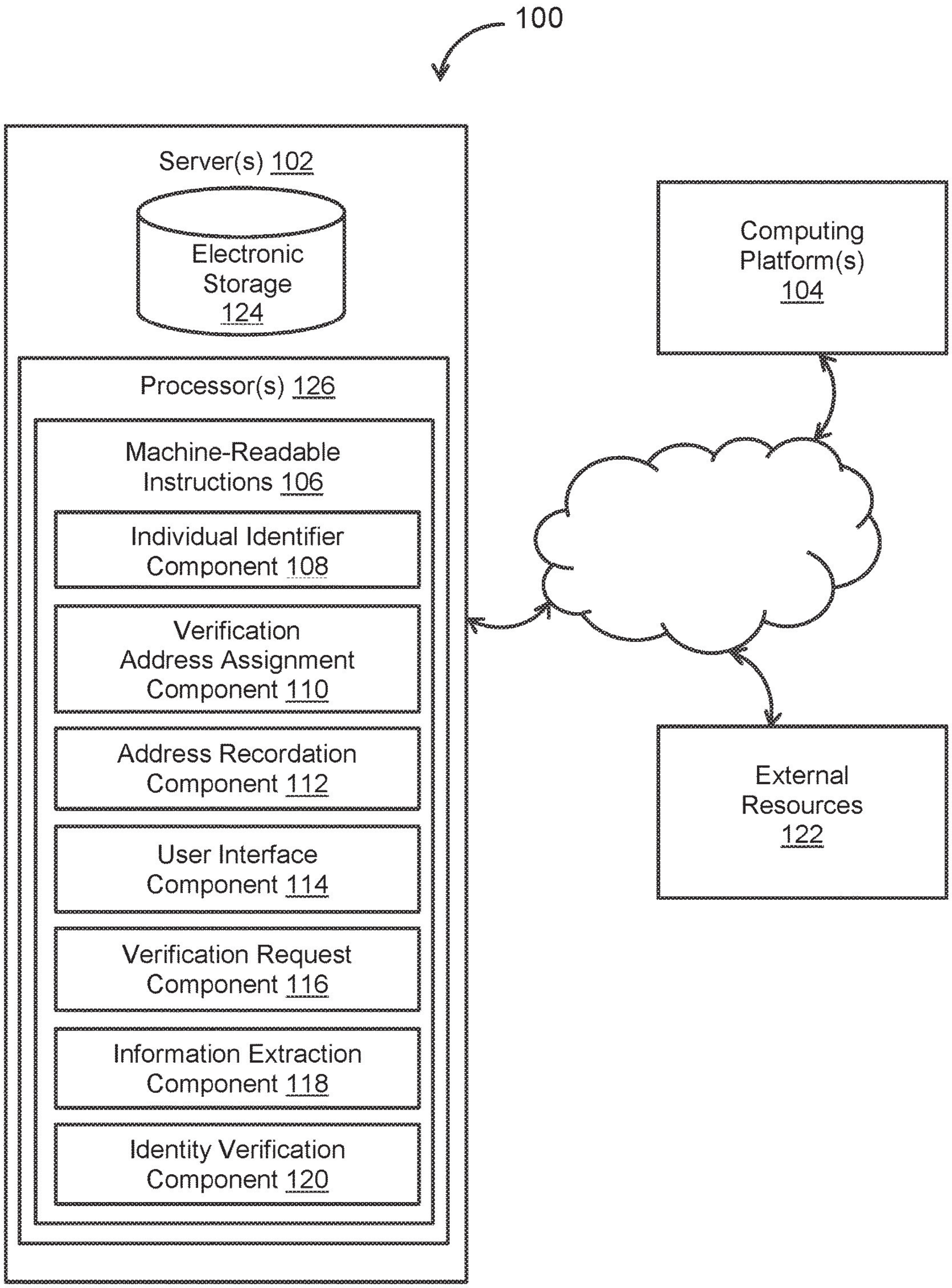

100
Server(s) 102
Electronic Storage 124
Processor(s) 126
Machine-Readable Instructions 106
Individual Identifier Component 108
Verification Address Assignment Component 110
Address Recordation Component 112
User Interface Component 114
Verification Request Component 116
Information Extraction Component 118
Identity Verification Component 120
Computing Platform(s) 104
External Resources 122

FIG. 1

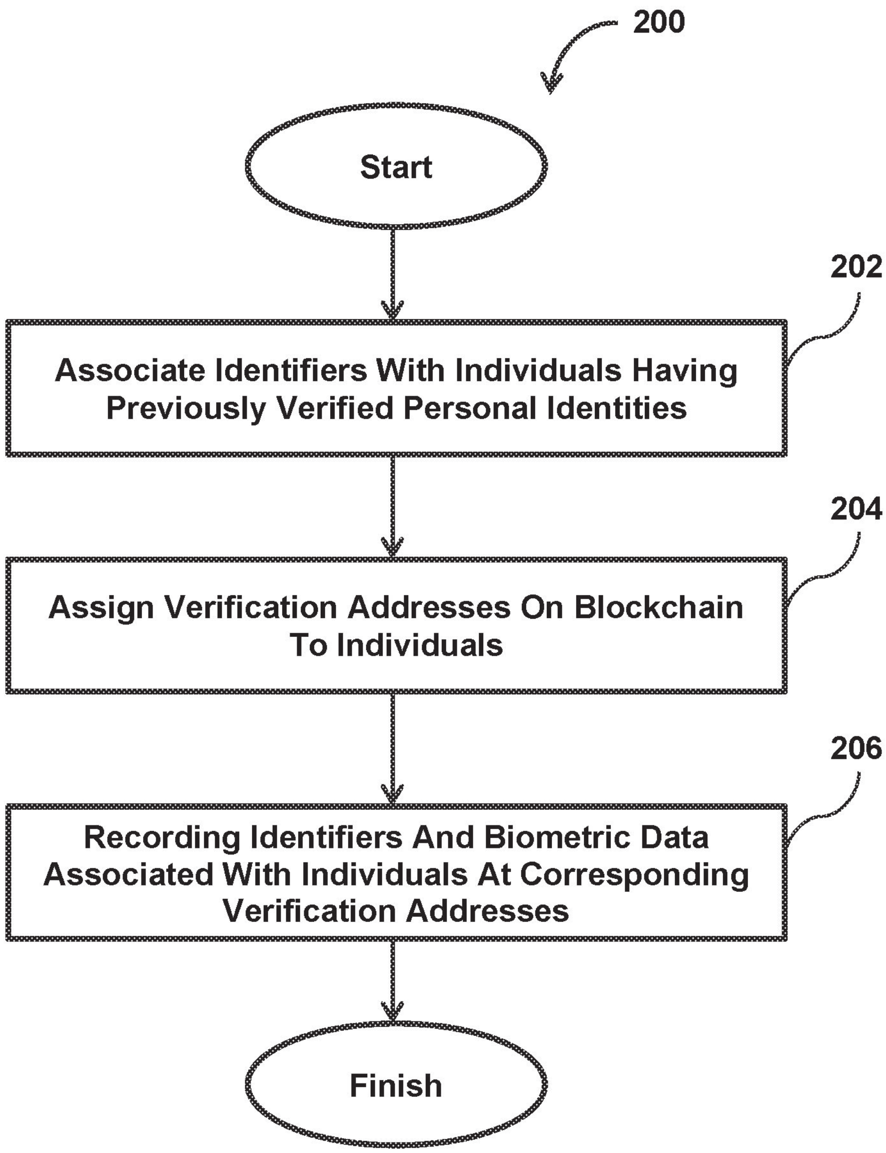

200
Start
202
Associate Identifiers With Individuals Having Previously Verified Personal Identities
204
Assign Verification Addresses On Blockchain To Individuals
206
Recording Identifiers And Biometric Data Associated With Individuals At Corresponding Verification Addresses
Finish

FIG. 2

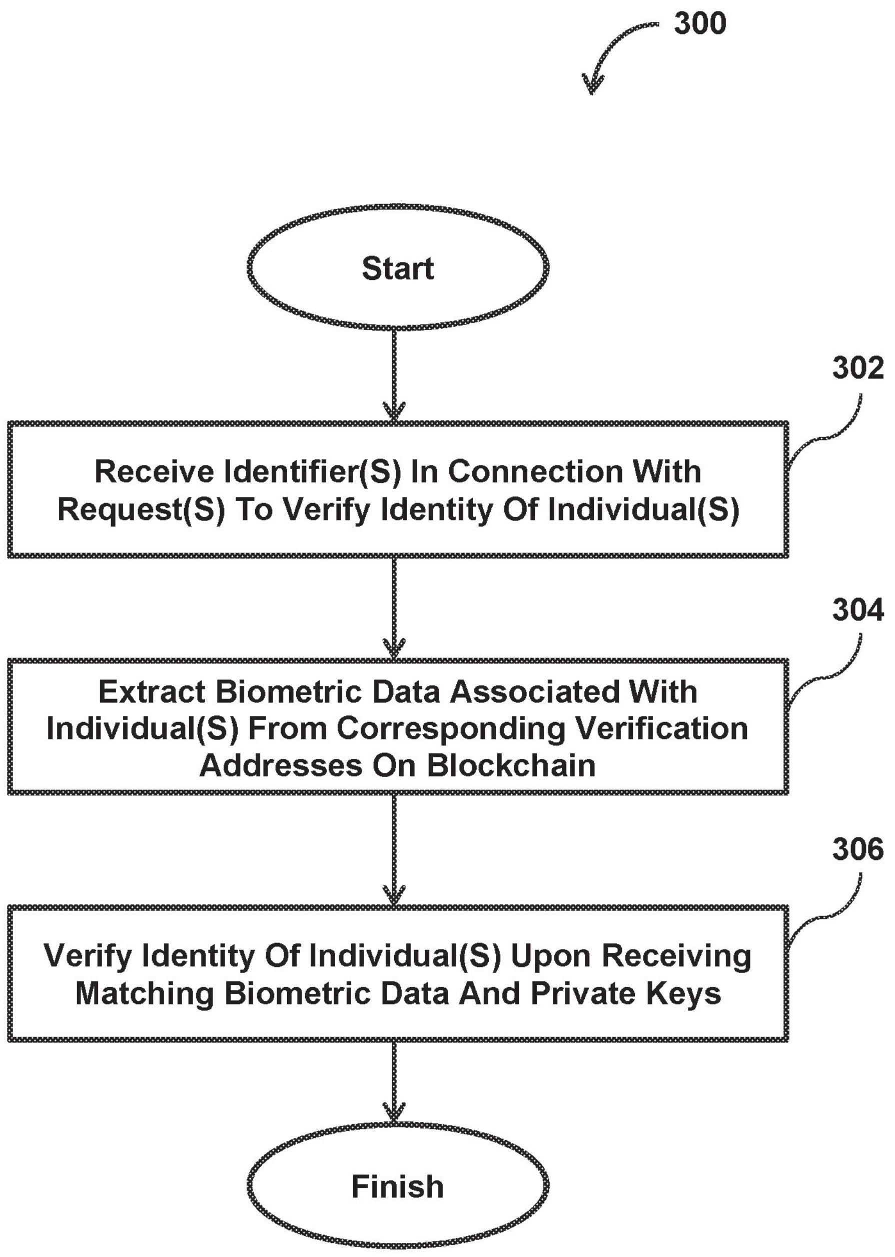

300
Start
302
Receive Identifier(S) In Connection With Request(S) To Verify Identity Of Individual(S)
304
Extract Biometric Data Associated With Individual(S) From Corresponding Verification Addresses On Blockchain
306
Verify Identity Of Individual(S) Upon Receiving Matching Biometric Data And Private Keys
Finish

FIG. 3

SYSTEMS AND METHODS FOR PROVIDING BLOCK CHAIN-BASED MULTIFACTOR PERSONAL IDENTITY VERIFICATION

FIELD OF THE DISCLOSURE

This disclosure relates to systems and methods for providing block chain-based multifactor personal identity verification.

SUMMARY

One aspect of the disclosure relates to a system for providing block chain-based multifactor personal identity verification. The system may include one or more hardware processors configured by machine-readable instructions to establish verification addresses on a block chain and/or perform block chain-based multifactor personal identity verification using the verification addresses. Establishing verification addresses on the block chain may include associating identifiers with individuals having previously verified personal identities, a first identifier being associated a first individual, the first individual having a previously verified personal identity; assigning verification addresses on a block chain to the individuals, a given verification address including a public key and a private key, a first verification address being assigned to the first individual, the first verification address including a first public key and a first private key; and recording identifiers and biometric data associated with the individuals at corresponding verification addresses, the first identifier and first biometric data associated with the first individual being recorded at the first verification address. Performing block chain-based multifactor personal identity verification using the verification addresses may include receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals, the first identifier being received in connection with a request to verify an identity of the first individual; extracting the biometric data associated with the one or more individuals from the corresponding verification addresses, the first biometric data associated with the first individual being extracted from the first verification address; and verifying the identity of the one or more individuals upon receiving matching biometric data and private keys, the personal identity of the first individual being verified upon receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key.

Another aspect of the disclosure relates to a method for establishing verification addresses on a block chain in order to provide block chain-based multifactor personal identity verification. The method may be performed by one or more hardware processors configured by machine-readable instructions. The method may include associating identifiers with individuals having previously verified personal identities, a first identifier being associated a first individual, the first individual having a previously verified personal identity; assigning verification addresses on a block chain to the individuals, a given verification address including a public key and a private key, a first verification address being assigned to the first individual, the first verification address including a first public key and a first private key; and recording identifiers and biometric data associated with the individuals at corresponding verification addresses, the first identifier and first biometric data associated with the first individual being recorded at the first verification address.

The identity of the one or more individuals may be verifiable upon receiving matching biometric data and private keys, such that the personal identity of the first individual is verifiable upon receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key.

Yet another aspect of the disclosure relates to a method for perform block chain-based multifactor personal identity verification using verification addresses. The method may be performed by one or more hardware processors configured by machine-readable instructions. The method may include receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals, a first identifier being received in connection with a request to verify an identity of a first individual; extracting biometric data associated with the one or more individuals from corresponding verification addresses on a block chain, a given verification address including a public key and a private key, first biometric data associated with the first individual being extracted from a first verification address assigned to the first individual, the first verification address including a first public key and a first private key; and verifying the identity of the one or more individuals upon receiving matching biometric data and private keys, the personal identity of the first individual being verified upon receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key.

These and other features, and characteristics of the present technology, as well as the methods of operation and functions of the related elements of structure and the combination of parts and economies of manufacture, will become more apparent upon consideration of the following description and the appended claims with reference to the accompanying drawings, all of which form a part of this specification, wherein like reference numerals designate corresponding parts in the various figures. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only and are not intended as a definition of the limits of the invention. As used in the specification and in the claims, the singular form of "a", "an", and "the" include plural referents unless the context clearly dictates otherwise.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** illustrates a system for providing block chain-based multifactor personal identity verification, in accordance with one or more implementations.

FIG. **2** illustrates a method for establishing verification addresses on a block chain in order to provide block chain-based multifactor personal identity verification, in accordance with one or more implementations.

FIG. **3** illustrates a method for performing block chain-based multifactor personal identity verification using verification addresses, in accordance with one or more implementations.

DETAILED DESCRIPTION

FIG. **1** illustrates a system **100** for providing block chain-based multifactor personal identity verification, in accordance with one or more implementations. In some implementations, system **100** may include one or more servers **102**. The server(s) **102** may be configured to communicate with one or more computing platforms **104** according to a client/server architecture, a peer-to-peer architecture, and/or other architectures. The users may access system **100** via computing platform(s) **104**.

The server(s) **102** may be configured to execute machine-readable instructions **106**. The machine-readable instructions **106** may include one or more of an individual identifier component **108**, a verification address assignment component **110**, an address recordation component **112**, a user interface component **114**, a verification request component **116**, an information extraction component **118**, an identity verification component **120**, and/or other machine-readable instruction components.

The machine-readable instructions **106** may be executable to establish verification addresses on a block chain. Generally speaking, a block chain is a transaction database shared by some or all nodes participating in system **100**. Such participation may be based on the Bitcoin protocol, Ethereum protocol, and/or other protocols related to digital currencies and/or block chains. A full copy of the block chain contains every transaction ever executed in an associated digital currency. In addition to transactions, other information may be contained by the block chain, such as described further herein.

The block chain may be based on several blocks. A block may include a record that contains and confirms one or more waiting transactions. Periodically (e.g., roughly every one minute), a new block including transactions and/or other information may be appended to the block chain. In some implementations, a given block in the block chain contains a hash of the previous block. This may have the effect of creating a chain of blocks from a genesis block (i.e., the first block in the block chain) to a current block. The given block may be guaranteed to come chronologically after a previous block because the previous block's hash would otherwise not be known. The given block may be computationally impractical to modify once it is included in the block chain because every block after it would also have to be regenerated.

A given verification address may include a specific location on the block chain where certain information is stored. In some implementations, an individual verification address may be referred to as an "AtenVerify Address." Verification addresses are further described below in connection with verification address assignment component **110**.

The individual identifier component **108** may be configured to associated identifiers with individuals having previously verified personal identities. For example, a first identifier may be associated a first individual. The first individual may have a previously verified personal identity. Generally speaking, an identifier may include one or more of a number, an alphanumeric code, a username, and/or other information that can be linked to an individual. In some implementations, an individual identifier may be referred to as an "Aten ID."

In accordance with some implementations, an individual having a previously verified personal identity may have obtained the previously verified personal identity through a variety of approaches. For example, in some implementations the individual may be required to provide evidence of the individual's identity. Such evidence may include one or more of providing a copy of a government issued identification (e.g., passport and/or driver's license), providing a copy of mail received by the individual (e.g., a utility bill), evidence provided by a third party, and/or other evidence on an individual's identity. The evidence may be provided to an entity associated with server(s) **102**.

The verification address assignment component **110** may be configured to assign verification addresses on a block chain to the individuals. A given verification address may include a public key and a private key. By way of example, a first verification address may be assigned to the first individual. The first verification address may include a first public key and a first private key.

Generally speaking, a public and private key-pair may be used for encryption and decryption according to one or more public key algorithms. By way of non-limiting example, a key pair may be used for digital signatures. Such a key pair may include a private key for signing and a public key for verification. The public key may be widely distributed, while the private key is kept secret (e.g., known only to its proprietor). The keys may be related mathematically, but calculating the private key from the public key is unfeasible.

In some implementations, verification address assignment component **110** may be configured such that private keys may be stored within computing platform(s) **104**. For example, the first private key may be stored within a computing platform **104** and/or other locations associated with the first individual. In accordance with some implementation, a private key may be stored in one or more of a "verify.dat" file, a SIM card, and/or other locations.

In some implementations, verification address assignment component **110** may be configured such that multiple verification addresses may be assigned to separate individuals. For example, in addition to the first verification address, a second verification address may be assigned to the first individual. One or more additional verification addresses may be assigned to the first individual, in accordance with one or more implementations.

The address recordation component **112** may be configured to record identifiers and biometric data associated with the individuals at corresponding verification addresses. For example, the first identifier and first biometric data associated with the first individual may be recorded at the first verification address. Recording information at a given verification address may include recording a hash or other encrypted representation of the information. In some implementations, different biometric data may be recorded at multiple verification addresses assigned to a single given individual. For example, in addition to the first identifier and the first biometric data associated with the first individual being recorded at the first verification address, the first identifier and second biometric data associated with the first individual may be recorded at a second verification address.

Generally speaking, biometric data may include metrics related to human characteristics. Biometric identifiers are distinctive, measurable characteristics that can be used to label and describe individuals. Biometric identifiers are typically include physiological characteristics, but may also include behavioral characteristics and/or other characteristics. Physiological characteristics may be related to the shape of an individual's body. Examples of physiological characteristics used as biometric data may include one or more of fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor or scent, and/or other physiological characteristics. Behavioral characteristics may be related to a pattern of behavior of an individual. Examples of behavioral characteristics used as biometric data may include one or more of typing rhythm, gait, voice, and/or other behavioral characteristics.

The biometric data may include one or more of an image or other visual representation of a physiological characteristic, a recording of a behavioral characteristic, a template of a physiological characteristic and/or behavioral characteristic, and/or other biometric data. A template may include a synthesis of relevant features extracted from the source. A template may include one or more of a vector describing features of a physiological characteristic and/or behavioral characteristic, a numerical representation of a physiological characteristic and/or behavioral characteristic, an image with particular properties, and/or other information.

Biometric data may be received via computing platforms **104** associated with the individuals. For example, biometric data associated with a first individual may be received via a first computing platform **104** associated with the first individual. The first computing platform **104** may include an input device (not depicted) configured to capture and/or record a physiological characteristic and/or behavioral characteristic of the first individual. Examples of such an input device may include one or more of a camera and/or other imaging device, a fingerprint scanner, a microphone, an accelerometer, and/or other input devices.

The user interface component **114** may be configured to provide an interface for presentation to individuals via associated computing platforms **104**. The interface may include a graphical user interface presented via individual computing platforms **104**. According to some implementations, the interface may be configured to allow a given individual to add or delete verification addresses assigned to the given individual so long as at least one verification address is assigned to the given individual.

In some implementations, user interface component **114** may be configured to access and/or manage one or more user profiles and/or user information associated with users of system **100**. The one or more user profiles and/or user information may include information stored by server(s) **102**, one or more of the computing platform(s) **104**, and/or other storage locations. The user profiles may include, for example, information identifying users (e.g., a username or handle, a number, an identifier, and/or other identifying information), security login information (e.g., a login code or password), system account information, subscription information, digital currency account information (e.g., related to currency held in credit for a user), relationship information (e.g., information related to relationships between users in system **100**), system usage information, demographic information associated with users, interaction history among users in the system **100**, information stated by users, purchase information of users, browsing history of users, a computing platform identification associated with a user, a phone number associated with a user, and/or other information related to users.

The machine-readable instructions **106** may be executable to perform block chain-based multifactor personal identity verification using the verification addresses.

The verification request component **116** may be configured to receive one or more identifiers in connection with one or more requests to verify an identity of one or more individuals. For example, the first identifier may be received in connection with a request to verify an identity of the first individual. Requests for identity verification may be provided in connection with and/or related to financial transactions, information exchanges, and/or other interactions. Requests may be received from other individuals and/or other third parties.

The information extraction component **118** may be configured to extract the biometric data associated with the one or more individuals from the corresponding verification addresses. For example, the first biometric data associated with the first individual may be extracted from the first verification address. Extracting information (e.g., biometric data) from a verification address may include decrypting information.

According to some implementations, information extraction component **118** may be configured such that, responsive to receiving the request to verify the identity of the first individual, a prompt may be provided to the first individual for biometric data matching the first biometric data and a private key matching the first private key. The prompt may be conveyed via a computing platform **104** associated with the first individual. The prompt may be conveyed via a graphical user interface and/or other user interface provided by the computing platform **104** associated with the first individual. The prompt may include an indication that is one or more of visual, audible, haptic, and/or other indications.

In some implementations, information extraction component **118** may be configured such that, responsive to receiving the request to verify the identity of the first individual, a prompt may be provided to a computing platform **104** associated with the first individual. The prompt may cause the computing platform **104** to automatically provide, to server(s) **102**, biometric data matching the first biometric data and/or a private key matching the first private key.

The identity verification component **120** may be configured to verify the identity of the one or more individuals upon, or in response to, receiving matching biometric data and private keys. For example, the personal identity of the first individual may be verified upon receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key. Verifying the personal identity of the first individual may include comparing stored information with newly received information.

According to some implementations, identity verification component **120** may be configured such that the personal identity of the first individual may be verified upon receipt of (1) biometric data matching the first biometric data or the second biometric data and (2) a private key matching the first private key. Such implementations may provide so-called "M-of-N" signatures for identity verification where some subset of a larger set of identifying information is required.

In some implementations, identity verification component **120** may be configured such that the biometric data matching the first biometric data and the private key matching the first private key may be used to sign the verification of the personal identity of the first individual.

A cryptographic signature is a mathematical mechanism that allows someone to prove ownership. In the case of Bitcoin, a Bitcoin wallet and its private key(s) are linked by some mathematical magic. When your Bitcoin software signs a transaction with the appropriate private key, the whole network can see that the signature matches the bitcoins being spent. However, there is no way for the world to guess your private key to steal your hard-earned bitcoins.

In some implementations, at least one dedicated node performs the signing of the verification of the personal identity of the first individual. A given dedicated node may include one or more of the server(s) **102**. The given dedicated node may be a public node or a private node configured for creating new blocks and/or for signing verification.

In some implementations, server(s) **102**, computing platform(s) **104**, and/or external resources **122** may be operatively linked via one or more electronic communication links. For example, such electronic communication links may be established, at least in part, via a network such as the Internet and/or other networks. It will be appreciated that this is not intended to be limiting, and that the scope of this disclosure includes implementations in which server(s) **102**, computing platform(s) **104**, and/or external resources **122** may be operatively linked via some other communication media.

A given computing platform **104** may include one or more processors configured to execute machine-readable instructions. The machine-readable instructions may be configured to enable an expert or user associated with the given computing platform **104** to interface with system **100** and/or external resources **122**, and/or provide other functionality attributed herein to computing platform(s) **104**. By way of non-limiting example, the given computing platform **104** may include one or more of a desktop computer, a laptop computer, a handheld computer, a tablet computing platform, a NetBook, a Smartphone, a gaming console, and/or other computing platforms.

External resources **122** may include sources of information, hosts and/or providers of virtual environments outside of system **100**, external entities participating with system **100**, and/or other resources. In some implementations, some or all of the functionality attributed herein to external resources **100** may be provided by resources included in system **100**.

Server(s) **102** may include electronic storage **124**, one or more processors **126**, and/or other components. Server(s) **102** may include communication lines, or ports to enable the exchange of information with a network and/or other computing platforms. Illustration of server(s) **102** in FIG. **1** is not intended to be limiting. Server(s) **102** may include a plurality of hardware, software, and/or firmware components operating together to provide the functionality attributed herein to server(s) **102**. For example, server(s) **102** may be implemented by a cloud of computing platforms operating together as server(s) **102**.

Electronic storage **124** may comprise non-transitory storage media that electronically stores information. The electronic storage media of electronic storage **124** may include one or both of system storage that is provided integrally (i.e., substantially non-removable) with server(s) **102** and/or removable storage that is removably connectable to server(s) **102** via, for example, a port (e.g., a USB port, a firewire port, etc.) or a drive (e.g., a disk drive, etc.). Electronic storage **124** may include one or more of optically readable storage media (e.g., optical disks, etc.), magnetically readable storage media (e.g., magnetic tape, magnetic hard drive, floppy drive, etc.), electrical charge-based storage media (e.g., EEPROM, RAM, etc.), solid-state storage media (e.g., flash drive, etc.), and/or other electronically readable storage media. Electronic storage **124** may include one or more virtual storage resources (e.g., cloud storage, a virtual private network, and/or other virtual storage resources). Electronic storage **124** may store software algorithms, information determined by processor(s) **126**, information received from server(s) **102**, information received from computing platform(s) **104**, and/or other information that enables server(s) **102** to function as described herein.

Processor(s) **126** may be configured to provide information processing capabilities in server(s) **102**. As such, processor(s) **126** may include one or more of a digital processor, an analog processor, a digital circuit designed to process information, an analog circuit designed to process information, a state machine, and/or other mechanisms for electronically processing information. Although processor(s) **126** is shown in FIG. **1** as a single entity, this is for illustrative purposes only. In some implementations, processor(s) **126** may include a plurality of processing units. These processing units may be physically located within the same device, or processor(s) **126** may represent processing functionality of a plurality of devices operating in coordination. The processor(s) **126** may be configured to execute machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, **120**, and/or other machine-readable instruction components. Processor(s) **126** may be configured to execute machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, **120**, and/or other machine-readable instruction components by software; hardware; firmware; some combination of software, hardware, and/or firmware; and/or other mechanisms for configuring processing capabilities on processor(s) **126**. As used herein, the term "machine-readable instruction component" may refer to any component or set of components that perform the functionality attributed to the machine-readable instruction component. This may include one or more physical processors during execution of processor readable instructions, the processor readable instructions, circuitry, hardware, storage media, or any other components.

It should be appreciated that although machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, and **120** are illustrated in FIG. **1** as being implemented within a single processing unit, in implementations in which processor(s) **126** includes multiple processing units, one or more of machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, and/or **120** may be implemented remotely from the other machine-readable instruction components. The description of the functionality provided by the different machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, and/or **120** described below is for illustrative purposes, and is not intended to be limiting, as any of machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, and/or **120** may provide more or less functionality than is described. For example, one or more of machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, and/or **120** may be eliminated, and some or all of its functionality may be provided by other ones of machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, and/or **120**. As another example, processor(s) **126** may be configured to execute one or more additional machine-readable instruction components that may perform some or all of the functionality attributed below to one of machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, and/or **120**.

FIG. **2** illustrates a method **200** for establishing verification addresses on a block chain in order to provide block chain-based multifactor personal identity verification, in accordance with one or more implementations. The operations of method **200** presented below are intended to be illustrative. In some implementations, method **200** may be accomplished with one or more additional operations not described, and/or without one or more of the operations discussed. Additionally, the order in which the operations of method **200** are illustrated in FIG. **2** and described below is not intended to be limiting.

In some implementations, one or more operations of method **200** may be implemented in one or more processing devices (e.g., a digital processor, an analog processor, a digital circuit designed to process information, an analog circuit designed to process information, a state machine, and/or other mechanisms for electronically processing information). The one or more processing devices may include one or more devices executing some or all of the operations of method **200** in response to instructions stored electronically on an electronic storage medium. The one or more processing devices may include one or more devices configured through hardware, firmware, and/or software to be specifically designed for execution of one or more of the operations of method **200**.

At an operation **202**, identifiers may be associated with individuals having previously verified personal identities. A first identifier may be associated a first individual. The first individual may have a previously verified personal identity. Operation **202** may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to individual identifier component **108** (as described in connection with FIG. **1**), in accordance with one or more implementations.

At an operation **204**, verification addresses on a block chain may be assigned to the individuals. A given verification address may include a public key and a private key. A first verification address may be assigned to the first individual. The first verification address may include a first public key and a first private key. Operation **204** may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to verification address assignment component **110** (as described in connection with FIG. **1**), in accordance with one or more implementations.

At an operation **206**, identifiers and biometric data associated with the individuals may be recorded at corresponding verification addresses. The first identifier and first biometric data associated with the first individual may be recorded at the first verification address. The identity of the one or more individuals may be verifiable upon, or in response to, receiving matching biometric data and private keys. The personal identity of the first individual may be verifiable upon, or in response to, receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key. Operation **206** may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to address recordation component **112** (as described in connection with FIG. **1**), in accordance with one or more implementations.

FIG. **3** illustrates a method **300** for performing block chain-based multifactor personal identity verification using verification addresses, in accordance with one or more implementations. The operations of method **300** presented below are intended to be illustrative. In some implementations, method **300** may be accomplished with one or more additional operations not described, and/or without one or more of the operations discussed. Additionally, the order in which the operations of method **300** are illustrated in FIG. **3** and described below is not intended to be limiting.

In some implementations, method **300** may be implemented in one or more processing devices (e.g., a digital processor, an analog processor, a digital circuit designed to process information, an analog circuit designed to process information, a state machine, and/or other mechanisms for electronically processing information). The one or more processing devices may include one or more devices executing some or all of the operations of method **300** in response to instructions stored electronically on an electronic storage medium. The one or more processing devices may include one or more devices configured through hardware, firmware, and/or software to be specifically designed for execution of one or more of the operations of method **300**.

At an operation **302**, one or more identifiers may be received in connection with one or more requests to verify an identity of one or more individuals. A first identifier may be received in connection with a request to verify an identity of a first individual. Operation **302** may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to verification request component **116** (as described in connection with FIG. **1**), in accordance with one or more implementations.

At an operation **304**, biometric data associated with the one or more individuals may be extracted from corresponding verification addresses on a block chain. A given verification address may include a public key and a private key. First biometric data associated with the first individual may extracted from a first verification address assigned to the first individual. The first verification address may include a first public key and a first private key. Operation **304** may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to information extraction component **118** (as described in connection with FIG. **1**), in accordance with one or more implementations.

At an operation **306**, the identity of the one or more individuals may be verified upon, or in response to, receiving matching biometric data and private keys. The personal identity of the first individual may be verified upon, or in response to, receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key. Operation **306** may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to identity verification component **120** (as described in connection with FIG. **1**), in accordance with one or more implementations.

Exemplary implementations may facilitate storing personal data on the block chain. The personal data may be stored on the block chain in an encrypted way. A person may be identified at the block chain level with one or more of a private key, a finger print, a finger print hash, an eye retina, an eye retina hash, and/or other unique information. The data stored may include or relate to one or more of a passport, an identification card, extracted passport information, a driver's license, extracted driver's license information, finger print, eye retina, and/or other information. According to some implementations, if some of the data is changed, a new record may be created for that person in the block chain. That is, all changes are added as new records. The old record will always be stored on the block chain. Generally speaking, all records on the block chain are stored forever and cannot be removed. More than one copy of the block chain will exist to ensure the records are not manipulated.

Exemplary implementations may facilitate access to personal data. There may be multiple access levels for the personal data in the block chain. Access controls may be grated on public/private key pairs levels. Examples of access levels may include one or more of Super Admin (full access to block chain), Authorities-country level (full read-only access), Authorities-state/local level (limited read-only access), Police and other services including Emergency (access to certain personal data by Finger Print/Eye retina of that person only), Participating Merchants (limited access), and/or other access levels.

Exemplary implementations may facilitate verification check. There may be multiple levels for how it is possible to check verification. For example, some implementations may ensure a person has a record at "Company" but no personal data is provided. Some implementations may ensure a person has a record at Company and get very basic personal information such as Full Name, DOB, Gender, and/or other basic information. Some implementations may ensure a person has a record at Company and get all personal data.

Although the present technology has been described in detail for the purpose of illustration based on what is currently considered to be the most practical and preferred implementations, it is to be understood that such detail is solely for that purpose and that the technology is not limited to the disclosed implementations, but, on the contrary, is intended to cover modifications and equivalent arrangements that are within the spirit and scope of the appended claims. For example, it is to be understood that the present technology contemplates that, to the extent possible, one or more features of any implementation can be combined with one or more features of any other implementation.

What is claimed is:

1. A system for providing blockchain-based multifactor personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain;

a server-side computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the server-side computer system to:

assign a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity;

store, at the one or more computer-readable storage media, an identifier of the individual and a biometric hash of the individual in association with the verification address associated with the blockchain,

wherein the biometric hash is a hash of biometric data of the individual, and

wherein each of the identifier, the biometric hash, and the verification address are different from one another and different from private and public keys from which the verification address was derived;

obtain, from a client-side device, the identifier and the biometric data in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain;

obtain the stored identifier and the stored biometric hash using the verification address indicated in the request; and

sign verification of the individual's identity responsive to a determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

2. The system of claim **1**, wherein the server-side computer system is caused to:

sign, using the private key from which the verification address was derived, the verification of the individual's identity responsive to the determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

3. The system of claim **2**, wherein the server -side computer system is caused to:

store, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;

obtain, from the client-side device, the private key in connection with the request to verify the individual's identity;

obtain the stored private key using the verification address indicated in the request; and

sign, using the private key, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, and the private key of the request match the stored identifier, the stored biometric hash, and the stored private key.

4. The system of claim **3**, wherein the private key is also stored on the client-side device, and wherein the client-side device is a user device of the individual.

5. The system of claim **1**, wherein the server-side computer system is caused to:

assign another verification address associated with the blockchain to the individual;

store, at the one or more computer-readable storage media, another biometric hash of the individual in association with the other verification address associated with the blockchain, the other biometric hash being a hash of other biometric data of the individual;

obtain, from the client-side device, the other biometric data in connection with the request to verify the individual's identity, the request further indicating the other verification address associated with the blockchain;

obtain the stored other biometric hash using the other verification address indicated in the request; and

sign the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, the other biometric data of the request match the stored identifier, the stored biometric hash, and the stored other biometric hash.

6. The system of claim **5**, wherein the server-side computer system is caused to:

obtain, via a user interface, a user-initiated command to add the other verification address as an address of the blockchain for the individual; and

assign the other verification address associated with the blockchain to the individual based on the user-initiated command.

7. The system of claim **5**, wherein the server-side computer system is caused to:

obtain, via a user interface, a user-initiated command to remove the other verification address as an address of the blockchain for the individual; and

de-associate the other verification address associated with the blockchain from the individual based on the user-initiated command.

8. The system of claim **1**, wherein the server-side computer system is caused to:

provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and

denying a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

9. The system of claim **1**, wherein the biometric data comprises an image, a recording, or a template.

10. The system of claim **1**, wherein the biometric data is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, or voice.

11. A method of providing blockchain-based multifactor personal identity verification, the method being implemented by a server-side computer system comprising one or more processors executing computer program instructions that, when executed, perform the method, the method comprising:

storing, by the server-side computer system, a blockchain at one or more computer-readable storage media of the server-side computer system;

assigning, by the server-side computer system, a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity;

storing, by the server-side computer system, at the one or more computer-readable storage media, an identifier of the individual and a biometric hash of the individual in association with the verification address associated with the blockchain,

wherein the biometric hash is a hash of biometric data of the individual, and

wherein each of the identifier, the biometric hash, and the verification address are different from one another and different from private and public keys from which the verification address was derived;

obtaining, by the server-side computer system, from a client-side device, the identifier and the biometric data in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain;

obtaining, by the server-side computer system, the stored identifier and the stored biometric hash using the verification address indicated in the request; and

assigning, by the server-side computer system, verification of the individual's identity responsive to a determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

12. The method of claim **11**, comprising:

signing, by the server-side computer system, using the private key from which the verification address was derived, the verification of the individual's identity responsive to the determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

13. The method of claim **12**, comprising:

storing, by the server-side computer system, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;

obtaining, by the server-side computer system, from the client-side device, the private key in connection with the request to verify the individual's identity;

obtain the stored private key using the verification address indicated in the request; and

signing, by the server-side computer system, using the private key, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, and the private key of the request match the stored identifier, the stored biometric hash, and the stored private key.

14. The method of claim **11**, comprising:

assigning, by the server-side computer system, another verification address associated with the blockchain to the individual;

storing, by the server-side computer system, at the one or more computer-readable storage media, another biometric hash of the individual in association with the other verification address associated with the blockchain, the other biometric hash being a hash of other biometric data of the individual;

obtaining, by the server-side computer system, from the client-side device, the other biometric data in connection with the request to verify the individual's identity, the request further indicating the other verification address associated with the blockchain;

obtaining, by the server-side computer system, the stored other biometric hash using the other verification address indicated in the request; and

signing, by the server-side computer system, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, the other biometric data of the request match the stored identifier, the stored biometric hash, and the stored other biometric hash.

15. The method of claim **14**, comprising:

obtaining, by the server-side computer system, via a user interface, a user-initiated command to add the other verification address as an address of the blockchain for the individual; and

assigning, by the server-side computer system, the other verification address associated with the blockchain to the individual based on the user-initiated command.

16. The method of claim **14**, comprising:

obtaining, by the server-side computer system, via a user interface, a user-initiated command to remove the other verification address as an address of the blockchain for the individual; and

de-associating, by the server-side computer system, the other verification address associated with the blockchain from the individual based on the user-initiated command.

17. The method of claim **11**, comprising:

providing, by the server-side computer system, a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and

denying, by the server-side computer system, a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

18. The method of claim **11**, wherein the biometric data comprises an image, a recording, or a template.

19. The method of claim **11**, wherein the biometric data is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, or voice.

20. A system for providing blockchain-based multifactor personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain;

a server-side computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the server-side computer system to:

assign multiple verification addresses of the blockchain to the individual, the individual having a previously verified personal identity, the multiple verification addresses include a first verification address associated with the blockchain and a second verification address associated with the blockchain;

store, at the one or more computer-readable storage media, (i) an identifier of the individual and a first biometric hash of the individual in association with the first verification address associated with the blockchain and (ii) a second biometric hash of the individual in association with the second verification address associated with the blockchain,

wherein the first biometric hash is a hash of first biometric data of the individual, and the second biometric hash is a hash of second biometric data of the individual, and

wherein each of the identifier, the first biometric hash, the second biometric hash, the first verification address, and the second verification address are different from one another, different from first private and public keys from which the first verification address was derived, and different from second private and public keys from which the second verification address was derived;

obtain, from a client-side device, the identifier, the first biometric data, and the second biometric data in connection with a request to verify the individual's identity, the request indicating the first verification address associated with the blockchain and the second verification address associated with the blockchain;

obtain (i) the stored identifier and the stored first biometric hash using the first verification address

indicated in the request and (ii) the stored second biometric hash using the second verification address indicated in the request; and

sign, using the private key from which the first verification address was derived, verification of the individual's identity responsive to a determination that the identifier of the request, the first biometric data of the request, and the second biometric data of the request match the stored identifier, the stored first biometric hash, and the stored second biometric hash;

provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the first verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the first verification address was derived and different from the private key from which the second verification address was derived; and

deny a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

* * * * *

Exhibit 4

From: Ben Boyer
Sent: Wednesday, February 7, 2018 3:33 PM PST
To: jdillman@blockbits.capital
Subject: FW: Intros

He could actually be a CEO candidate, if he got excited. He's super dialed into commerce and financial services. He's a total curmudgeon but an amazing manager.

From: Benjamin Boyer <ben@tenayacapital.com>
Date: Wednesday, February 7, 2018 at 3:29 PM
To: Reed Taussig <rtaussig@threatmetrix.com>, "jdillman@blockbits.capital" <jdillman@blockbits.capital>
Subject: Intros

Hi Japheth,
Per our previous conversation, please meet Reed Taussig. Reed is the CEO of ThreatMetrix, which is an amazing Tenaya portfolio company in the fraud space which just came to terms on a sale to Relix.
https://www.threatmetrix.com/press-releases/

I mentioned to Reed your interest in speaking with him and he kindly offered to take the introduction.

I'll let you take it from here.

-Ben

Ben Boyer
MANAGING DIRECTOR

TENAYA CAPITAL
O 650.687.6523
E ben@tenayacapital.com

3280 Alpine Road
Portola Valley, CA 94028
TENAYACAPITAL.COM

Exhibit 5

From:	Ben Boyer
Sent:	Sunday, April 29, 2018 10:16 AM PDT
To:	Japheth Dillman
CC:	Arthur Weissman
Subject:	Re: Any update?

Btw, I have a cousin that works at the FBI. He said there's a large financial crimes team that's focused on ICOs that don't launch. Obviously it hasn't been that long but if an investigation is ever launched publicly, this coin will be worthless.

From: Benjamin Boyer <ben@tenayacapital.com>
Date: Sunday, April 29, 2018 at 10:09 AM
To: Japheth Dillman <jdillman@blockbits.capital>
Cc: Arthur Weissman <arthur.weissman@gmail.com>
Subject: Re: Any update?

At best, they seem disorganized and at worst, dishonest. Not a great way to build trust and support ahead of the ICO

From: Japheth Dillman <jdillman@blockbits.capital>
Date: Sunday, April 29, 2018 at 9:55 AM
To: Benjamin Boyer <ben@tenayacapital.com>
Cc: Arthur Weissman <arthur.weissman@gmail.com>
Subject: Re: Any update?

Yes, I've seen that too. The glacial movement of the exchanges was entirely frustrating, I just had a call with Marcus where I told him no matter how frustrated he is in the delays, communications MUST be stronger to the community. He's prepping a PR now but I think he needs more comma

Sent from my iPhone

On Apr 29, 2018, at 9:53 AM, Ben Boyer <ben@tenayacapital.com> wrote:

> The lack of communication and transparency is disheartening.
>
> Telegram and AMLBitcoinTalk are both melting down.
>
> Even the most ardent supporters are starting to get nervous.

Exhibit 6

Gmail

Marcus Andrade <ceo@amlbitcoin.com>

As promised I outline my thinking below

1 message

David Cohen <davidcohenfamily@hotmail.com> Tue, Aug 20, 2019 at 12:18 PM
To: "Marcus Andrade (ceo@amlbitcoin.com)" <ceo@amlbitcoin.com>

Good morning Marcus,

As promised I outline my thinking on a proposed transaction below.

I realize that you want to make more money than is presently proposed to you. Undoubtedly, you have read stories about how Mark Zuckerberg (Facebook) turned down buy-out offers and went on to become one of the richest men in the world - thinking this could be you. I respect and appreciate people who have a dream, but there are times in life when one has to realize that a good chunk of a pie is better than no pie and starving. This is one of those times. In my personal business career as a leader and advisor to other very successful investors I have seen countless examples of founders missing key opportunities to sell only to end up regretting it for the rest of their lives. You never read about the tens of thousands of these failure stories but just about the one in a million stories which are more interesting.

On the table (or soon on the table, once we can get in there and make the offer real) is a potential $100 million buyout. The group is very real, and their interest is very real - contingent on their attorneys' due diligence.

I realize that, for some reason, you are angry at Jack, but angry people don't make deals - they usually blow them. So, I hope you can put emotion aside and look rationally at what's on the table.

At this time, as I understand it, you have no other serious funding options (other than whatever you can get from a loan against the house and other assets). You have no real, tangible prospect of a large investor coming to the rescue, enabling you to continue on your development path for this project. It is not productive at this point to get into the reasons why this is the case, but it is the case. The people who have been involved in this project who could have introduced you to major financing are not willing to do so at this time (other than Jack), so you are left with a great option on the table - but it's probably the only option.

If you take this option, and sell to this group, you will make a huge score, pay your creditors, satisfy your coin purchasers (including me), show the investigating authorities that this was not only not some fraud, but was a fantastic business proposition - with no room for any complaints since everyone will be satisfied.

If you wisely invest your family money (and I'm oversimplifying and treating your individual interest and your kids trust as collectively your family) - even if you were to receive $30,000,000-$40,000,000 and I believe it will be more than that - you could live the life of a very well off man, and take care of your family for several generations. You would also relieve the stress that must be tearing you apart inside.

You'll be the hero. The rich hero. You'll be sought after for advice and asked to participate in many other deals. Life would be great.

If you decide, however, to pass up this deal, there is no telling where things will go. The odds of you finding another major funding source while the coin trades at pennies, and while you have not been able to do anything yet with the patents are remote. And the prospect of the coin trading higher than this price are really remote as well - since there are no resources to capture the imagination of that community.

Obviously, as a significant coin holder, I want only the best for the project. I don't want to lose my money, as I am sure none of the coin holders want. A worst case scenario going forward would be a disaster for all of us, but you must come to realize that it is a far more likely scenario than you finding a large financial partner.

If you let this life preserver float away, for whatever reason, you can imagine on your own the possible bad outcomes several of which I have listed at the bottom of this email in blue.

I am in no way threatening you; I am trying to present you with possible outcomes so you can make a rational and unemotional decision.

If you opt to sell, you will have a company that has committed $100 million to buy the assets, and possibly another $100 million to turning the enterprise into a success. You will retain a large amount of digital currency that may enable you to achieve super wealth. And you won't have the stress and headaches and incur legal and other expenses to make that happen….the buyer will.

According to what I have read about them, the prospective buyer has been playing in the billions of dollars for a while, and according to Jack, they are keen to invest to make this into everything all of us ever hoped for. And you could win mightily if they do… but in the meantime, you will already be financially set even if they flop.

Speaking of Jack, I don't know why your relationship has fallen apart, but that is not important at this point. Love him or hate him, he has a life preserver in his hands for you. You are going to pay him for it, but you are going to benefit more than anyone and more than you have ever in your life.

As we discussed my understanding is you have agreed to compensate Jack with 30% of any gross proceeds from all of the three companies and I am proposing 10% for me. That leaves you and your family 60% before paying anyone else you need to pay. I am a respected business person used to dealing with very large and complex transactions. Deals are hard to get done and you will respect and appreciate the professionalism I will bring to a process and I believe my involvement and experience will maximize the chances of having a successful outcome and present potential additional upside for all.

If this is something you want to pursue I will take charge of such a process. However I am not interested in an exercise in futility so let’s discuss if you want to move forward or say no to this opportunity. If you do wish to move forward, you need to do so rapidly, or the opportunity will disappear on its own. Time skills all deals and this group is already wondering why this is taking so long.

Lastly thank you for taking the time to read this and considering my approach.

Regards

-David

David A. Cohen

Some possible bad outcomes include:

1. Some of the coin holders filing fraud actions in court.

2. Some of the creditors suing for past debts and seeking to attach assets to foreclose upon.

3. Perhaps one of the patent violators taking the project to court to undo the patents. While they may not succeed under normal circumstances, a full blown legal case is not something you have the resources for and people with resources beat people who have none almost always in civil court.

4. The federal investigation by the FBI moves from investigation to grand jury indictments, with the attendant publicity killing any chance for the project. At that point, no one will want to get anywhere near this.

5. The federal criminal tax investigation of you moves forward with the federal government seizing the patents and your other companies and assets under their asset forfeiture laws - all in advance of obtaining a ruling against you, but enough to put the blood in the water for your competitors.

6. You completely run out of money and are forced to put the project and your companies into bankruptcy. Some people see bankruptcy as a protection, but this is not always the case. In fact, the court appointed trustee would be in charge, and likely move to fire sale assets to pay creditors and coin holders.

Gmail **Marcus Andrade <ceo@amlbitcoin.com>**

ack is on a plane but I wanted to send you this.

David Cohen <davidcohenfamily@hotmail.com> ed, Aug 28, 2019 at 11: PM
To: Marcus Andrade <ceo@amlbitcoin.com>

Marcus, I am sending this to you. ac is on a lane until tomorro afternoon. I have some thoughts. I reali e this is a long email, and you robably don t ant to read it all, but I strongly encourage you to do so.

e both no ho much a sale of this ro ortion ill hel you (and all of us). The ros ect of you having enough money to defend yourself fully against la enforcement, as ell as live the rest of your life ith financial security should be a huge motivation for you. hen you add in the fact that doing a huge deal roves to your detractors that you ere right all along, and settles and satisfies those ho invested money in you and your dream, losing this deal is a very bad idea.

I reali e that there are those telling you that a better deal ill come along, or some other nonsense. Marcus, no one in this deal has done as many deals as I have. The rice these guys are illing to ay you is e traordinary. Fran ly, I don t no of anyone ho ould ay such a remium at this stage of develo ment.

But the bigger issue is that, even if there ere a better deal do n the road in a fe years, can you really last that long financially Are there funds lining u to rovide you money Ho soon before you ve finally e hausted all sources of funds As I understand it, none of those ho, in the ast, have come to your financial rescue (including me) are illing to do any more ith you on this ro ect.

And hat ha ens if the IRS or the Do decide to ursue asset forfeiture even before you are convicted of or lead to anything (ithout the money re uired to mount a defense against the federal government) They do that all the time, as you might no . If they do so here, the ro ect is dead. o one ill get any here near this ro ect. The assets (atents and anything else) ill be fro en ending the outcome of your case. If you lead or are convicted, they ill sell your assets (all your assets) at a sheriff s sale, and someone else ill scoo them u , ithout you getting a dime.

And hy is this ha ening Because you are a arently listening to a atent la yer and a securities la yer. They have one interest: getting fees out of you. That s it. The ros ect that you are selling your ro ect means that the Marcus gravy train is coming to a halt for them. So, they are giving you terrible advice, because their interests are not aligned ith yours.

And hat is this advice For you to ma e it im ossible for anyone to hel you negotiate the best deal ossible. ac and I ant to ma e this or and ma e it big, not because it ill only benefit you. But because it ill benefit us. Do you thin e ant a smaller deal Hell no. e ant the best e can get from these buyers, so e all ma e as much money as ossible.

hen you demand, as your la yers a arently have on your behalf, that ac (and I, resumably) agree to have this deal terminated because the offer he resents might not fit your resent conce tion of hat you ant, you are guaranteeing failure. o deal starts out the ay you ant it. you have to or ith the other arty to com romise and get hat you both are satisfied ith. I reali e that your la yers have no clue about ho to do deals, but I find it very hard to believe that they are so dense as to thin anyone ould agree to the terms you have demanded of ac .

I heard from ac that you told him you, someho , have ut your attorneys into a veto osition over this deal. I imagine that s ust something you told him to negotiate, because hy ould anyone do such a thing ven if they ut u 2 0,000, you ouldn t give them control of the deal. I ut u 200,000. I didn t as for control of the deal. Ho could it be that someone ith of 1 interest in this deal (that s hat it is at 100,000,000) can no control the deal

And ho could it be that they ould be so utterly unreasonable, if it is in fact they ho are demanding these terms The only e lanation is that they are trying to tan the deal so they can continue suc ing money out of you, or accruing fees o ed so they can one day foreclose on you and ta e these assets for themselves. Don t id yourself, Marcus. I ve seen a lot orse.

So, ac is on a lane. hen he hits LA, he is going to call the buyers and set u a meeting for Friday morning (that s hat he told me before he too off). hen that ha ens, the deal is dead. There is no coming bac , unless you later go begging ac to someho rene discussions because you are, erha s in a fe ee s, in a real death inch. At that oint, do you actually believe ac is going to settle for 0 , assuming he does it at all He ll li ely offer you 0 and ho no s hat ill be ha ening at that oint you might have to ta e it.

I thin you need to thin really hard about hat you are doing. I thin the a roach you have ta en has led you to the brin of losing this deal. In my vie , you should sign the signed agreement he sent to you and let us get on ith this. If not, I no he is going to end this, and e ill all go our se arate ays.

It s your call. You once mentioned that you didn t ant to face the day hen you had to tell your grandchildren that you sold a billion dollar deal for 100,000,000. Ho ill you e lain things to them if you gave u a huge deal for no deal Or orse.
Let s get this signed and a deal done.
David

David A. Cohen

From: Ben Boyer
Sent: Thursday, February 22, 2018 8:26 AM EST
To: jdillman@blockbits.capital <jdillman@blockbits.capi
Subject: Fwd: Briefing: Growing ICO Unease

If interested, feel free to join this call under my subscription.

Ben Boyer
Managing Director
Tenaya Capital
3280 Alpine Road
Portola Valley, CA
94028
Tel: (650) 687-6523
Fax: (650) 687-6524
www.tenayacapital.com

From: The Information <info@theinformation.com>
Sent: Wednesday, February 21, 2018 7:00:52 PM
To: ben.boyer@gmail.com
Subject: Briefing: Growing ICO Unease

BRIEFING

Our views on the day's tech news.

F

What Happens to Crypto Assets (Fortune)

F

F

Now Publishers Talking to Ama (Digiday)

F

Google Once Again Pitching An
(The
Information)

F

Apple Is Hungry for Cobalt (Bloomberg)

Airbnb “Experiences” Had Slug
(The Wall Street
Journal)

F

Sling No Substitute for Dish’ (The Information)

Layoffs at Vox (BuzzFeed)

F

Uber Expands ‘Express Pool’ (Gizmodo

Priceline Group is Now Bookin
(The
Information)

Spotify Co-Founders to Mainta
(Bloomberg)

LATEST ARTICLES FROM THE INFORMATION

EXCLUSIVE

Cisco Close to Picking New Gl

By Kevin McLaughlin and Sarah Kuranda 21, 2018 We

The Biggest Tech Investor Sil

By Serena Saitto · Wednesday Feb 21, 2018

FOLLOW US

Sent to ben.boyer@gmail.com | Unsubscribe | Help

The Information · 100 First Street, San Francisco, CA 94

MANUEL A. MEDRANO, (SBN 102802)
mmedrano@zuberlawler.com
Zuber Lawler LLP
350 S. Grand Avenue, 32nd Floor
Los Angeles, California 90071 USA
Telephone: +1 (213) 596-5620
Facsimile: +1 (213) 596-5621

BRIAN BECK (*pro hac vice*, IL BN 6310979)
Zuber Lawler LLP
135 S. LaSalle St., Suite 4250
Chicago, Illinois 60603
Tel: (312) 346-1100
Fax: (213) 596-5621
bbeck@zuberlawler.com

Attorneys for Defendant Rowland Marcus Andrade
[Additional counsel listed on the next page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. ROWLAND MARCUS ANDRADE, Defendant.	Case No. 3:20-cr-00249-RS ORDER Granting Ex Parte Motion of Defendant Rowland Marcus Andrade to Issue Subpoena to Tenaya Capital, Inc.

On March 4, 2021, the defendant Rowland Marcus Andrade, represented by counsel, filed an *ex parte* motion to issue a subpoena to Tenaya Capital, Inc. pursuant to Fed. R. Crim. P. 17(c) and Criminal Local Rule 17-2(a)(1). For good cause shown, Defendant's motion is hereby GRANTED. IT IS HEREBY ORDERED that the Clerk's Office shall issue the Subpoena attached as Exhibit 1 to the Declaration of Brian J. Beck in support of Defendant's motion, and defense counsel shall be responsible for service of the Subpoena upon the third-party.

DATED: Macrh 4, 2021

HONORABLE RICHARD SEEBORG
Chief United States District Judge

MAURICIO S. BEUGELMANS (Bar No. 201131)
Murphy & McGonigle, RLLP
44 Montgomery Street, Suite 3750
San Francisco, CA 94104
Tel: (415) 651-5707
Fax: (415) 651-5708
mbeugelmans@mmlawus.com

LIONEL ANDRÉ (*pro hac vice*, DC BN 422534)
Murphy & McGonigle, P.C.
1001 G Street NW, 7th Floor
Washington, DC 20001
Tel: (202) 661-7039
Fax: (202) 661-7059
landre@mmlawus.com

KATHERINE D. COOPER (*appearance pro hac vice*)
Murphy & McGonigle, P.C.
1185 Avenue of the Americas, 21st Floor
New York, NY 10036
Tel: (212) 880-3630
Fax: (212) 880-3998
kcooper@mmlawus.com

Attorneys for Defendant Rowland Marcus Andrade